MICROSEC
Software Engineering & Consulting Ltd.

White Paper

The Next Generation Authentication Solution

September 8, 2014

PassBy[ME]

The Next Generation Authentication Technology

In a Nutshell

PassBy[ME] (PBM) is a **third generation authentication solution**[1] that can be used in any online environment where authenticating the user and establishing its true identity is highly important. These services include the financial industry, governments as well as a number of cloud-based services. As online services and transactions grow across the entire landscape of the Internet, the establishment of the legitimate identity behind these transactions has become a top priority.

With every passing day, we conduct more and more of our own personal and business affairs on the Internet. And it is not just the regular stuff like online banking, or webmail. Home alarm systems, TV sets, company cloud resources and very soon our cars are all hooked up onto the Internet doing various things. Our private network of Internet based things, the number and type of services we use show an incredible growth. Major risks associated also come with this trend.

Online fraud and identity theft are becoming a major threat to the online services world. Whoever controls our identity, also controls our private network and a large part of our lives along with it. Financial risks and e-commerce losses associated are biting into the 50 billion dollar range and growing steadily. The rise of identity theft has reached alarming levels and fear of illegitimate access to cloud based services are becoming an everyday reality. Large organizations like governments, financial institutions, cloud service providers are doing everything they can to defend their own perimeters by implementing encryption and fraud prevention techniques. However, they largely leave the end user, the customer, without secure authentication. The online services and e-commerce world is only as secure as the weakest link in it. Customer behavior is a substantial risk to the online services landscape and it is proven to be the weakest link with the majority of online attacks coming through the customers' interaction. The message is clear. Experts now say that customer authentication needs to be strengthened in order to make the online world a safer place and provide grounds for further online services growth.

[1] Forrester Report: Navigate the Future of Identity and Access Management - Eve Maler, April 7, 2014

PassBy[ME]

To provide an answer to authentication related security concerns, we have developed PassBy[ME] as a state-of-the-art authentication service. It is a customer friendly, ergonomic, yet extremely secure authentication solution where Public Key Infrastructure (PKI) provides for the highest level of security known today and mobile devices create the smooth customer experience. PassBy[ME] strengthens customer authentication, the weakest link in the chain of online transactions today.

PassBy[ME] is available as a service or packaged solution. It provides the mobile-based second factor leg of an authentication scheme already implemented by an online service provider (e.g. online banking or cloud service login-password). It eliminates costly hardware tokens and/or sms messages. Its unique messaging system is not only very fast but has the capability to provide signed receipts of messages as proof of delivery.

PassBy[ME] is a real two-factor, easy-to-use, smart phone based[2], universal and portable identification and authentication technology. It is a 3rd generation authentication solution following suite of the 2nd generation of tokens and OTPs[3]. The solution exploits the smart devices' PKI ability as a second factor security device. PassBy[ME] eliminates costly SMS text messages or the usage of one-time-password generating devices like tokens. PKI technology is recognized today to be the highest possible security standard.

PassBy[ME] will work well with Access and ID Management systems as their authentication module. PBM creates a traceable access method through certificates and certificate management.

PassBy[ME] uses international security standards, protocols and interfaces such as PKI or SCEP to provide transparency, trust and easy integration. The PassBy[ME] system works both as a service or an integrated product. Integration times vary and may be as little as a few days in case of the service.

PassBy[ME] as a service is designed to handle minimum amount of customer information, which may be as little as a unique identifier of a customer. The PassBy[ME] system does not store and handle sensitive customer information, financial information and other confidential information. It focuses solely on the secure authentication of an identity.

The unique market differentiator and value added of the PassBy[ME] system is that it is a universally portable authentication method in high security environments such as e-banking or e-government.

[2] Android, iOS, BlackBerry, Windows
[3] One-Time-Passwords

MAIN FEATURES

- General -

- Available as a service or a packaged product for larger deployments.
- Is designed to provide a second factor authentication to an already existing authentication scheme e.g. username-password scenario.
- Mobile based with free mobile app.
- Mobile development SDK is provided for branded apps.
- Excellent customer experience.
- Easy user enrollment & management.
- Online Management Dashboard.
- Fast messaging system to provide signed receipts of messages delivered.

- Security -

- Uses PKI[3] with corresponding keys and certificates. The keys are generated „on board" the device and impossible to copy or export.
- Additional key protection available using pin codes or passswords.
- Two-device two-channel authentication scheme where PBM provides for the second device and second channel.
- Standardized technology – we do not believe in security through obscurity.
- Increased security to second generation authentication technology e.g. OTPs.[4]
- No sensitive customer information is transferred through the system.

- Cost -

- Makes use of the BYOD[5] scheme – this eliminates additional hardware token cost.
- Uses its own messaging system by default and thus eliminates third party telecommunications charges like sms text or audio call.
- Affordable montly fees even for the smallest of comapnies.

- Implementation -

- Easy set-up and easy user management.
- Thanks to the standardized technology, implementation takes a few days only.
- Service availability is 99.9%

[4] Public Key Infrastructure
[5] Bring Your Own Device

Use Cases

The following are possible use cases for PassBy[ME]. The list may not be complete due to the diversity of authentication requirements.

- FINANCIAL SECTOR -

Online Banking Access

PassBy[ME] completes the current security measures already established in the online banking and payment environments by substantially strengthening customer authentication, the weakest link in the security chain. As the second factor authentication leg, PassBy[ME] exploits the advantages of BYOD[6] scenario. OTPs are thus eliminated so are the associated costs of sms messages and the inconveniences of additional hardware tokens. Threats such as MITM[7], Phishing and other malware are eliminated.

Credit Card Usage & Online Payments

Fraud is becoming an ever-growing threat to the financial integrity of payment systems. PassBy[ME] can be used in case of online credit card purchases. E-Commerce is losing a lot of business due to CNP[8] fraud. Losses are also attributed to fraud prevention systems being too strict and stopping otherwise legitimate transactions. PassBy[ME] blends into this environment by providing and easy-to-use authentication scheme to secure credit card purchases. Even if the card information is stolen, a PassBy[ME] enabled customer will have no worries as no card transaction will be authorized without PBM authentication. The biggest advantage of this is that e-commerce merchants are not involved and they do not have to make modifications to their websites. In the case of MasterCard Secure Code (3D Secure) and Verified By Visa, PassBy[ME] provides the authentication module to these payment transactions as well.

PassBy[ME] will boost customer confidence in no-cash payments and will significantly reduce financial losses resulting from online fraud.

Card Present & ATM Cash Withdrawal

In these scenarios, PassBy[ME] may be required to provide for a safe authentication in addition to pin codes in case of higher spending or cash withdrawal limits. The customer will require Internet access and this may be an inconvenience. The same would not apply to online transactions as they are by default online and Internet access is assumed.

[6] Bring Your Own Device
[7] Man-In-The-Middle or Man-In-The-Browser
[8] Card Not Present

- E-GOVERNMENT –

e-Government services are on the rise. More and more citizens and businesses have access to a growing number of e-government services. Since most of these transactions involve confidential information, sensitive data and documents, authentication has become a top priority. Also, governments like the idea of a generally usable authentication method. With PassBy[ME], they can have a fully universal and mobile authentication based on PKI keys and certificates and can establish the true identity of a user. With usage of certificates and other personal attributes, PBM is fit to service all aspects of e-government services:

- **e-health** services to access medical records, prescriptions, applications
- **Business Services to corporations** – business formation services, access to records, applications, copies of good standing, change information related to a business, submission of due records and reports.
- **Tax services** – submitting tax records, accessing tax accounts, submitting change of information, managing tax issues, etc.
- **Citizen Services** – driver's licence, reistered address, immigration accounts, building permits, unemployment registration, etc.
- **Internal government access** – PBM will enable government workers and high ranking officials to access government databases and confidential documents in a secure and traceable way.

- CLOUD SERVICE PROVIDERS -

More and more cloud services are available in the Cloud. They are both for internal use within one company (VPN, company databases, CRM systems, etc.) or to the average user such as webmail (e.g. Hotmail), storage services (e.g. Dropbox), remote computer access services (e.g. LogMeIn), CRM and Sales Services (e.g. Salesforce.com). Cloud providers are doing everything they can to encrypt and protect information from fraudulent access. But the fact is, that they usually offer very basic forms of authentication to their customers. It is no surprise that most of the fraudulent access attempts target the end-user itself and steal login credentials and access confidential information.

PassBy[ME] is a logical choice for cloud service providers to integrate it as authentication module. With the BYOD scheme, it is very simple and integration will take very little amount of time and resources.

PassBy[ME] would be an essential component to ID & Access Management systems as well to provide the authentication module to these services.

How PassBy[ME] Works – Online Payment Example

The solution is based on a true two-factor (both the devices and channels are separate) authentication method over the Internet. It is made possible by the evolution of the smart devices where these devices are now capable of generating and using high-level PKI cryptography technology. The security feature of the PassBy[ME] system relies on Public Key Infrastructure with the corresponding 2048 bit private keys. This makes smart phones highly effective security devices.

Each customer receives his or her private key generated on the smart device. No additional device is needed. The private key is generated and stored on the smart device. This guarantees that the private key exists in only one copy, hence the security feature. In an e-Commerce scenario, when making an online purchase for example, the customer will initiate the transaction by giving his or her credit card information online as it is done today. The payment provider bank will then validate the transaction by requesting a second authentication through the smart phone, which is independent from the device used for the online transaction. The PassBy[ME] system comes with a built-in (or stand alone) mobile application that can be branded and integrated into any payment provider's own mobile application. When initiating an online transaction on one device – a PC for example – the customer will receive an alert on his mobile device and a request to authenticate the transaction. The customer will be able to confirm or reject the transaction. If there is no mobile app of the payment provider on its own, the PassBy[ME] system provides its own app. The bank or the payment provider will only authorize the transaction if the customer authentication was successful and the customer confirmed the online transaction.

Any number of customer mobile devices can be personalized, including tablets. Personalizing the smart device is an automatic and quick process and will take only a few minutes at a bank branch. Stolen or lost devices are reported much the same way as stolen or lost credit cards. Upon reporting such a loss, the certificates are revoked immediately making it impossible for the device to authorize further transactions.

By using PKI keys and certificates, a very flexible user management is possible. On the management dashboard, users' certificates can be revoked if stolen, or reinstated if recovered safe. This saves money in the banking sector, as there is no need to reproduce credit cards and there is no inconvenient hassle for the customer to get a new card.

Watch the PassBy[ME] Video to show you all this in 2 minutes:

PASSBY[ME]

The PassBy[ME] Team

PassBy[ME] technology was developed by an international group of IT Security Experts, PKI specialists and consultants with the contribution of e-government and online payment experts. The PassBy[ME] System was developed by Microsec e-Szigno Qualified Certificate Authority, Hungary, Europe.

Standards and Compliances

PassBy[ME] is built on and/or complies with the following main industry standards and recommendations:

- Payment Card Industry Data Security Standard (PCI DSS)
- MasterCard Site Data Protection Program (SDP)
- VISA Cardholder Information Security Program (CISP)
- Federal Financial Institutions Examinations Council, USA (FFIEC Internet Authentication guidance)
- PKI – Public Key Infrastructure
- rfc 5280 - Internet X.509 Public Key Infrastructure Certificate and CRL Profile
- rfc 2560 - X.509 Internet Public Key Infrastructure Online Certificate Status Protocol (OCSP)
- rfc 4043 - Internet X.509 Public Key Infrastructure Permanent Identifier
- rfc 5246 - The Transport Layer Security (TLS) Protocol
- SCEP - Simple Certificate Enrollment Protocol draft-nourse-scep-23
- NTC 3161 – Internet X509 Public Key Infrastructure, Time-Stamp Protocol (TSP)
- ETSI 101 903 V1.2.2, V1.3.2, XML Advanced Electronic Signatures (XAdES)
- SOAP – Simple Object Access Protocol
- MQ Telemetry Transport Protocol

Contact

For further information, please contact the PassBy[ME] team at:

info@passbyme.com

www.passbyme.com